

101522388
Rec'd PCT/PTO 25 JAN 2005

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
12. Februar 2004 (12.02.2004)

PCT

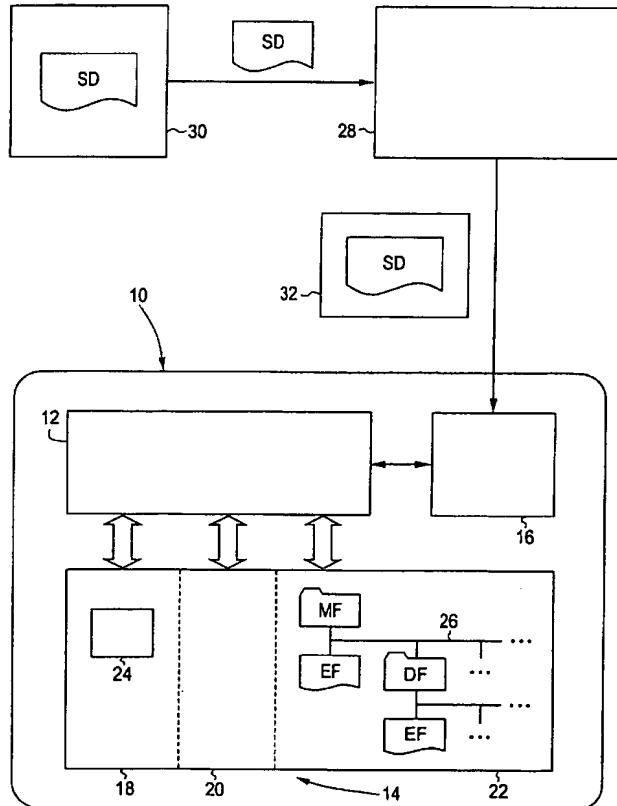
(10) Internationale Veröffentlichungsnummer
WO 2004/013821 A1

- (51) Internationale Patentklassifikation⁷: **G07F 7/10**, G06F 17/30, G06K 19/073
- (21) Internationales Aktenzeichen: PCT/EP2003/008121
- (22) Internationales Anmeldedatum: 24. Juli 2003 (24.07.2003)
- (25) Einreichungssprache: Deutsch
- (26) Veröffentlichungssprache: Deutsch
- (30) Angaben zur Priorität:
102 34 158.3 26. Juli 2002 (26.07.2002) DE
- (71) Anmelder (*für alle Bestimmungsstaaten mit Ausnahme von US*): **GIESECKE & DEVRIENT GMBH [DE/DE]**; Prinzregentenstrasse 159, 81677 München (DE).
- (72) Erfinder; und
- (75) Erfinder/Anmelder (*nur für US*): **CIESINGER, Daniel [DE/DE]**; Lily-Braun-Weg 15, 80639 München (DE). **MEISTER, Gisela [DE/DE]**; Stademannstr. 11, 81737 München (DE).
- (74) Anwalt: **DENDORFER, Claus**; Wächtershäuser & Hartz, European Patent and Trademark Attorneys, Weinstrasse 8, 80333 München (DE).

[Fortsetzung auf der nächsten Seite]

(54) Title: INSTALLATION OF A FILE SYSTEM IN A DATA SUPPORT

(54) Bezeichnung: EINRICHTEN EINES DATEISYSTEMS IN EINEM DATENTRÄGER



(57) Abstract: The invention relates to a method for installation of a file system (26) in a portable data support (10), comprising the following steps: inputting specification data (SD), which describes the file system (26) at least partly at the semantic level, the installed data specification (SD) is then interpreted by a processor centre (12) in the data support (10) and the file system (26) installed in a memory on the data support (10), according to the interpreted specification data (SD). A data support (30) which may be read by computer and a device for initialisation and or personalising a portable data support (10) are able to store specification data (SD), or to transfer the same to said portable data support (10). The invention provides the technology for installation of a file system (26) in a data support (10) which reduces the conventional high dependency on the file format employed and the internal operating system of the data support (10).

(57) Zusammenfassung: Ein Verfahren zum Einrichten eines Dateisystems (26) in einem tragbaren Datenträger (10) weist die Schritte auf, Spezifikationsdaten (SD), die das Dateisystem (26) zumindest zum Teil auf semantischer Ebene beschreiben, einzulesen, die eingelesenen Spezifikationsdaten (SD) durch einen Prozessorkern (12) des Datenträgers (10) zu interpretieren, und das Dateisystem (26) gemäß den interpretierten Spezifikationsdaten (SD) in einem Speicher (14) des Datenträgers (10) einzurichten. Ein computerlesbarer Datenträger (30) und eine Vorrichtung (28) zur Initialisierung und/oder Personalisierung eines tragbaren Datenträgers (10) sind dazu eingerichtet, Spezifikationsdaten (SD) zu speichern bzw. in einen erfindungsgemäßen tragbaren Datenträger (10) zu übertragen. Die Erfindung stellt eine Technik zum

[Fortsetzung auf der nächsten Seite]

WO 2004/013821 A1



(81) **Bestimmungsstaaten (national):** AE, AG, AL, AM, AT (Gebrauchsmuster), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (Gebrauchsmuster), CZ, DK (Gebrauchsmuster), DK, DM, DZ, EC, EE (Gebrauchsmuster), EE, ES, FI (Gebrauchsmuster), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(84) **Bestimmungsstaaten (regional):** ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Erklärung gemäß Regel 4.17:

- *hinsichtlich der Berechtigung des Anmelders, ein Patent zu beantragen und zu erhalten (Regel 4.17 Ziffer ii) für die folgenden Bestimmungsstaaten AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR,*

HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

Veröffentlicht:

- *mit internationalem Recherchenbericht*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Einrichten eines Dateisystems in einem Datenträger

Die Erfindung betrifft allgemein das technische Gebiet, ein Dateisystem in einem tragbaren Datenträger, wie z.B. einer Chipkarte oder einem Chip-

5 modul, einzurichten.

Bevor ein Datenträger einsatzbereit ist, muß in ihm ein Dateisystem eingerichtet werden. Dies geschieht typischerweise im Zuge der Initialisierung des Datenträgers, also beim Einspielen von Daten und/oder Programmen,

10 die für eine größere Anzahl von Datenträgern identisch sind. Mit diesem Einspielen von Daten werden auch die Strukturen und Attribute (Dateibaum, Leserechte usw.) des Dateisystems ganz oder teilweise festgelegt. Das Dateisystem kann auch bei anderen Fertigungsschritten eingerichtet werden, z.B. bei der Personalisierung, also dem Einspielen von
15 Daten, die für den Datenträger bzw. dessen späteren Benutzer individuell sind.

In der Norm ISO 7816 wird beschrieben, wie ein normgemäßes Dateisystem in Chipkarten angelegt werden kann. Insbesondere behandelt ISO 7816-9

20 den Befehl CREATE FILE, mit dem sich die einzelnen Dateien des Dateisystems und die dazugehörigen Dateiattribute sukzessive anlegen lassen. Die Parameter des Befehls CREATE FILE sind so gestaltet, daß Bitfolgen aus den an die Chipkarte übermittelten Daten unmittelbar, also ohne weitere Umsetzung, in einen Speicher der Chipkarte geschrieben werden.

25 Das genaue Format der zur Dateisystem-Initialisierung in die Chipkarte übertragenen Daten ist meist proprietär und kann von dem jeweiligen Betriebssystem der Karte abhängen. Dies gilt insbesondere dann, wenn die Karte gegenüber der genannten Norm Änderungen oder Weiter-
30 entwicklungen aufweist, aber auch in anderen Fällen, weil die Norm einen gewissen Interpretationsspielraum zuläßt. Überdies kommen zunehmend

Chipkarten zum Einsatz, deren Dateisystem nicht gemäß ISO 7816 initialisiert werden kann oder bei denen dies zumindest nicht üblich ist, wie z.B. die Java Card™.

- 5 Wegen der starken Maschinenorientierung der üblichen Formate sind zum Erstellen und Bearbeiten der Initialisierungsdaten spezielle Hilfsprogramme erforderlich, die ebenfalls an die jeweils verwendete Chipkarte und deren Betriebssystem angepaßt sein müssen. Ein derartiges Hilfsprogramm, das für das Chipkarten-Betriebssystem STARCOS® der Anmelderin zugeschnitten
10 ist, wird gegenwärtig unter der Bezeichnung STARMAG® vertrieben. Auch hier besteht das Problem, daß einerseits das STARMAG®-Programm nicht oder nur eingeschränkt für Chipkarten mit anderen Betriebssystemen verwendbar ist, und daß andererseits möglicherweise nützliche Funktionen anderer Programme nicht für STARCOS®-Chipkarten zur Verfügung stehen.

- 15 Die bislang genannten Probleme bestehen nicht nur im Hinblick auf das Format der in die Chipkarte zu übertragenden Daten, sondern ebenso im Hinblick auf das Datenformat, in dem die benötigten Informationen über das anzulegende Dateisystem einer Initialisierungs- und/oder Personalisierungsvorrichtung für Chipkarten übermittelt werden. Auch hier werden proprietäre Formate eingesetzt, die überdies von den jeweils zu bearbeitenden Chipkarten abhängen und spezielle Hilfsprogramme erfordern.

- 20 Die Erfindung hat die Aufgabe, die genannten Probleme ganz oder zum Teil zu lösen. Insbesondere soll durch die Erfindung eine Technik zum Einrichten eines Dateisystems in einem Datenträger bereitgestellt werden, die die bisherige starke Abhängigkeit zwischen dem verwendeten Dateiformat und Betriebssystem-Interna des Datenträgers verringert. In bevorzugten Ausgestaltungen sollen marktübliche Hilfsprogramme und Werkzeuge universell,

also im Zusammenhang mit Dateisystem-Einrichtungsdaten für die unterschiedlichsten Datenträger, einsetzbar sein.

Erfnungsgemäß wird diese Aufgabe ganz oder zum Teil gelöst durch ein

- 5 Verfahren mit den Merkmalen von Anspruch 1, einen tragbaren Datenträger gemäß Anspruch 8, eine Initialisierungs- und/oder Personalisierungs- vorrichtung nach Anspruch 9 und einen computerlesbaren Datenträger gemäß Anspruch 10. Die abhängigen Ansprüche definieren bevorzugte Ausgestaltungen der Erfindung.

10

Die Erfindung geht von der Kombination zweier Grundideen aus. Erstens werden Spezifikationsdaten verwendet, die das im Datenträger einzurichtende Dateisystem zumindest zum Teil auf semantischer Ebene beschreiben.

Zweitens werden diese Spezifikationsdaten von einem Prozessorkern des

- 15 Datenträgers interpretiert. In diesem Zusammenhang soll unter einer Interpretation stets eine gewisse Verarbeitung und Umwandlung der Daten verstanden werden. Ein unverändertes Einschreiben von empfangenen Bitfolgen in einen Speicher des Datenträgers ist im allgemeinen keine Interpretation in diesem Sinne.

20

Durch die Erfindung wird eine erhebliche Abstraktion von Einzelheiten des Datenträger-Betriebssystems erreicht. Dadurch, daß die Interpretation der Spezifikationsdaten durch den Datenträger selbst vorgenommen wird, brauchen externe Systeme keine Interna des Betriebssystems zu kennen,

- 25 sondern können vielmehr gleichermaßen im Zusammenhang mit unterschiedlichen Typen von Datenträgern verwendet werden. Es entfällt also die Notwendigkeit, Datenstrukturen in dem für die Ablage benötigten speziellen Format bereitzustellen. Die so erzielte technische Vereinheitlichung bewirkt erhebliche Einsparungen im Hinblick auf Geräte, Software und Ausbildung

von Mitarbeitern. Überdies steigt durch die Abkapselung interner Datenstrukturen die Sicherheit des Gesamtsystems gegen ungewollte Fehlkonfiguration oder absichtliche Manipulation.

- 5 Die Aufzählungsreihenfolge der Schritte in den Verfahrensansprüchen soll nicht als Einschränkung des Schutzbereichs verstanden werden. Es sind vielmehr Ausgestaltungen der Erfindung vorgesehen, bei denen diese Verfahrensschritte in anderer Reihenfolge oder ganz oder teilweise parallel oder ganz oder teilweise ineinander verzahnt (*interleaved*) ausgeführt werden.
- 10 Insbesondere werden in bevorzugten Ausgestaltungen die Spezifikationsdaten Stück für Stück oder in einem kontinuierlichen Strom in den Datenträger eingelesen und jeweils abschnittsweise interpretiert, wobei die bei der Interpretation ermittelten Teile des Dateisystems jeweils sofort in den Speicher des Datenträgers eingeschrieben werden.
- 15 In bevorzugten Ausgestaltungen der Erfindung beschreiben die Spezifikationsdaten die Dateien des Dateisystems und die zugehörigen Dateiattribute. Die Dateiattribute können Sicherheitseinstellungen, wie z.B. Lese-, Schreib- und Ausführungsrechte, und/oder Protokolleinstellungen, wie z.B. eine
- 20 Übertragung per *Secure Messaging* oder *Secure Sockets Layer (SSL)*, definieren. Ferner können die Spezifikationsdaten Relationen zwischen Dateien des Dateisystems angeben, z.B. die Relation, daß zwei Dateien ein Schlüsselpaar bilden, die Relation, daß eine Datei ein Zertifikat für einen Schlüssel darstellt, oder die Relation Datei/Eigentümer. Durch diese möglichen
- 25 Inhalte stellen die Spezifikationsdaten in bevorzugten Ausführungsformen ein mächtiges Beschreibungsmittel für das Dateisystem dar.

Die Spezifikationsdaten weisen bevorzugt ein textuelles und/oder portables und/oder interoperables Datenformat auf. Durch diese Maßnahmen lassen

sich Werkzeuge und Hilfsprogramme gleichermaßen für unterschiedliche Datenträger einsetzen. In manchen Ausgestaltungen werden weit verbreitete Standard-Datenformate eingesetzt, wie z.B. XML (*extensible markup language*), oder Formate entsprechend den Codierregeln DER (*distinguished encoding rules*) oder BER (*basic encoding rules*) oder PER (*packed encoding rules*), die für Datenstrukturen vorgesehen sind, welche in ASN.1 (*abstract syntax notation no. 1*) definiert sind.

Für standardisierte Datenformate wie die oben genannten steht eine Vielzahl von universell verwendbaren Werkzeugen zur Verfügung. Beispielsweise können Spezifikationsdaten im XML-Format mittels üblicher Web-Browser visualisiert werden. Auch sind derartige Formate vielen Entwicklungsingenieuren bereits bekannt, so daß keine aufwendigen Schulungen erforderlich sind. Die Spezifikationsdaten können in einer einzigen Datei zusammengefaßt sein oder in Form von mehreren Dateien vorliegen.

Die Spezifikationsdaten werden der Initialisierungs- oder Personalisierungsvorrichtung vorzugsweise bereits in demjenigen Format vorgelegt, in dem sie dann auch an den Datenträger übertragen werden. Eine solche Ausgestaltung hat den Vorteil, daß die Initialisierungs- oder Personalisierungsvorrichtung ohne oder mit nur geringem Einstellungsaufwand für unterschiedliche Datenträger einsetzbar ist. Insbesondere dann, wenn die Initialisierung oder Personalisierung von externen Dienstleistern vorgenommen wird, werden die Spezifikationsdaten vorzugsweise durch kryptographische Mittel, wie z.B. Verschlüsselung und/oder Signatur, gegen Manipulation und/oder Ausspähung geschützt. Die Entschlüsselung bzw. Prüfung der Signatur kann durch den Datenträger selbst vorgenommen werden, so daß außerhalb des Datenträgers keine Angriffsmöglichkeiten bestehen.

Der tragbare Datenträger, die Initialisierungs- und/oder Personalisierungs- vorrichtung und der computerlesbare Datenträger weisen in bevorzugten Weiterbildungen Merkmale auf, die den oben erwähnten und/oder den in den abhängigen Verfahrensansprüchen genannten Merkmalen entsprechen.

- 5 Der erfindungsgemäße computerlesbare Datenträger, der die Spezifikations- daten beinhaltet, braucht nicht notwendigerweise materieller Natur zu sein. Auch ein zur Datenübertragung geeignet moduliertes elektrisches oder elektromagnetisches Signal kann ein computerlesbarer Datenträger in diesem Sinne sein.

10

Weitere Merkmale, Aufgaben und Vorteile der Erfindung ergeben sich aus der folgenden Beschreibung mehrerer Ausführungsbeispiele und Ausführungsalternativen. Es wird auf die schematischen Zeichnungen verwiesen, in denen zeigen:

15

Fig. 1 ein Blockdiagramm von Komponenten, die an einem Ausführungs- beispiel des erfindungsgemäßen Verfahrens beteiligt sind, und

20 Fig. 2 eine beispielhafte Darstellung von Spezifikationsdaten, die als XML- Datei vorliegen.

In Fig. 1 ist ein tragbarer Datenträger 10 gezeigt, der beispielsweise als Chipkarte oder Chipmodul ausgebildet ist. In an sich bekannter Weise weist der Datenträger 10 einen Halbleiterchip auf, auf dem ein Prozessorkern 12, ein Speicher 14 und eine Schnittstelle 16 zur drahtgebundenen oder drahtlosen Kommunikation ausgebildet sind. Der Speicher 14 weist mehrere in unterschiedlichen Schaltungstechniken ausgebildete Bereiche auf, nämlich im vorliegenden Ausführungsbeispiel einen ROM-Bereich 18 mit maskenprogrammiertem Festwertspeicher, einen RAM-Bereich 20 mit flüchtigem

Schreib-/Lese-Speicher und einen Bereich 22 mit nicht-flüchtigem, wiederbeschreibbarem Speicher, z.B. EEPROM, Flash-Speicher usw.

- Der ROM-Bereich 18 des Speichers 14 enthält das Betriebssystem und die
- 5 von diesem Betriebssystem ausgeführten Programme des Datenträgers 10.
- Als Teil des Betriebssystems ist insbesondere ein Interpreter 24 vorgesehen, dessen Funktion später noch genauer erläutert werden wird. Ein Dateisystem 26 soll im EEPROM-Bereich 22 angelegt werden. In Fig. 1 ist zur Veranschaulichung ein Ausschnitt des Dateisystems 26 gezeigt, das der
- 10 Norm ISO 7816 entspricht und eine Wurzel MF (*master file*) sowie mehrere Hierarchieebenen von Verzeichnissen DF (*dedicated file*) und Einzeldateien EF (*elementary file*) aufweist. In Ausführungsvarianten wird das Dateisystem 26 gemäß anderen Konventionen oder Normen angelegt.
- 15 Der Datenträger 10 ist an eine Vorrichtung 28 angeschlossen, die zur Initialisierung und/oder Personalisierung des Datenträgers 10 dient. Die Vorrichtung 28 kann beispielsweise als an sich bekanntes Initialisierungssystem oder als Personalisierungssystem oder – in besonders einfachen Ausgestaltungen – als Computer mit einer geeigneten Schnittstelle zur Ankopplung an
- 20 den Datenträger 10 ausgestaltet sein. Die Vorrichtung 28 liest Spezifikationsdaten SD von einem computerlesbaren Datenträger 30 aus, der z.B. als Diskette oder CD-ROM ausgebildet sein kann. Die Spezifikationsdaten SD werden von der Vorrichtung 28 im vorliegenden Ausführungsbeispiel als Kommando-APDU (*application protocol data unit*) 32 an den Datenträger 10
- 25 übertragen.

Die Spezifikationsdaten SD enthalten eine Beschreibung des im Datenträger 10 anzulegenden Dateisystems 26 auf semantischer Ebene. Dies heißt im vorliegenden Ausführungsbeispiel, daß die Spezifikationsdaten SD die Struktur

des Dateisystems 26 sowie Dateiattribute und Beziehungen zwischen Dateien in einer abstrakten Form angeben, die von der Struktur der Bitfolgen der im Speicher 14 anzulegenden Verwaltungsdaten unabhängig ist. Die Spezifikationsdaten SD können als eine einzige Datei vorliegen oder auf 5 mehrere Dateien verteilt sein. Beispielsweise kann eine erste Spezifikationsdatei verwendet werden, um Benutzerinformationen anzulegen, eine zweite Spezifikationsdatei, um die Struktur des Dateisystems 26 zu erzeugen, eine Dritte, um Benutzer in Gruppen zusammenzufassen, und so weiter. In Ausgestaltungen, die mehrere 10 Spezifikationsdateien verwenden, werden bevorzugt entsprechend viele Kommando-APDUs 32 an den Datenträger 10 gesendet.

Ein Beispiel für Spezifikationsdaten SD, die in einem portablen und interoperablen XML-Format vorliegen, ist in Fig. 2 dargestellt. Die Dateitypen 15 MF, DF und EF des Dateisystems 26 werden hier durch entsprechende XML-Tags <MF ...>, <DF ...> und <EF ...> repräsentiert, und die Verschachtelung dieser Tags in den Spezifikationsdaten SD gibt die Baumstruktur des zu erzeugenden Dateisystems 26 an. Dateiattribute im Dateisystem 26 werden in den Spezifikationsdaten SD durch entsprechende XML-Attribute dargestellt. 20 So finden sich beispielsweise die grundlegenden Namensattribute FID (*file identifier*) und AID (*application identifier*) als XML-Attribute der Tags <DF ...> und <EF ...> wieder. Weitere XML-Attribute geben die Dateiart (*type*) und die maximale Dateigröße (*maxsize*) an.

25 In den Spezifikationsdaten SD werden im vorliegenden Ausführungsbeispiel ferner Sicherheitseinstellungen der einzelnen Dateien definiert, z.B. in Fig. 2 durch die XML-Attribute *access*, *owner*, *group* und *mode*. Schließlich werden auch Verknüpfungen zwischen Dateien definiert, z.B. in Fig. 2 durch das XML-Attribut *LinkTo*. In den Spezifikationsdaten SD können weitere Anga-

ben zu der anzulegenden Dateistruktur 26 oder zu anderen Initialisierungs- oder Personalisierungswerten für den Datenträger 10 enthalten sein. Einige Beispiele für derartige Angaben sind in Fig. 2 gezeigt.

- 5 Zur Initialisierung oder Personalisierung des Datenträgers 10 in dem System von Fig. 1 werden zunächst die Spezifikationsdaten SD erstellt. Wenn es sich um ein textuelles Datenformat handelt, kann dazu ein gewöhnlicher Texteditor dienen. Für andere strukturierte Datenformate kann ein geeignetes Werkzeug, beispielsweise ein XML-Generator, eingesetzt werden. Zur
10 Visualisierung kann ein üblicher Web-Browser dienen.

Die erstellten Spezifikationsdaten SD werden auf dem computerlesbaren Datenträger 30 gespeichert und von dort in die Initialisierungs- und/oder Personalisierungsvorrichtung 28 eingelesen. Im vorliegenden Ausführungs-
15 beispiel führt die Vorrichtung 28 keine inhaltliche Bearbeitung der Spezifikationsdaten SD durch, sondern "verpackt" diese Daten lediglich in einer geeigneten Kommando-APDU 32, die zum tragbaren Datenträger 10 übertragen wird.

- 20 Der Prozessorkern 12 des Datenträgers 10 empfängt die Kommando-APDU 32 über die Schnittstelle 16 und extrahiert die darin enthaltenen Spezifikationsdaten SD. Gesteuert vom Interpreter 24 interpretiert der Prozessorkern 12 die Spezifikationsdaten SD und legt das darin beschriebene Dateisystem 26 Stück für Stück im EEPROM-Bereich 22 des Speichers 14 an. Hierbei
25 werden die einzelnen Dateien erzeugt und die Dateiattribute einschließlich der Sicherheitseinstellungen entsprechend den interpretierten Spezifikationsdaten SD gesetzt. Ferner werden Relationen zwischen Dateien definiert und sonstige Einstellungen gemäß den Spezifikationsdaten SD vorgenommen.

Bei der Interpretation durch den Prozessorkern 12 werden im vorliegenden Ausführungsbeispiel unbekannte Elemente der Spezifikationsdaten SD, z.B. unbekannte XML-Tags, einfach ignoriert. Dadurch sind Ergänzungen oder

- 5 Erweiterungen des Formats der Spezifikationsdaten SD möglich, wobei auch Spezifikationsdaten SD im erweiterten Format von Datenträgern 10, die dieses Format nicht beherrschen, nach wie vor interpretiert werden können. Die strukturelle Identität der bekannten Elemente des Spezifikationsdaten-Formats geht also nicht verloren.

10

Die Spezifikationsdaten SD können auf dem computerlesbaren Datenträger 30 und/oder bei der Übertragung zum tragbaren Datenträger 10 in verschlüsselter und/oder signierter Form vorliegen. Die Entschlüsselung bzw. Signaturkontrolle findet dann erst im tragbaren Datenträger 10 statt. Da im

- 15 vorliegenden Ausführungsbeispiel die Vorrichtung 28 keine inhaltliche Veränderung der Spezifikationsdaten SD vornimmt, braucht hier keine Entschlüsselung zu erfolgen. Für den Initialisierungs- bzw. Personalisierungs- vorgang ist somit keine gesicherte Umgebung erforderlich.

Patentansprüche

1. Verfahren zum Einrichten eines Dateisystems (26) in einem tragbaren Datenträger (10), der einen Prozessorkern (12) und mindestens einen Speicher (14) aufweist, mit den Schritten:
 - Einlesen von Spezifikationsdaten (SD), die das Dateisystem (26) zumindest zum Teil auf semantischer Ebene beschreiben,
 - Interpretieren der eingelesenen Spezifikationsdaten (SD) durch den Prozessorkern (12), und
 - Einrichten des Dateisystems (26) gemäß den interpretierten Spezifikationsdaten (SD) in dem mindestens einen Speicher (14) des Datenträgers (10).
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Spezifikationsdaten (SD) die Dateistruktur des Dateisystems (26) einschließlich Dateiattributen beschreiben.
3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß die Dateiattribute Sicherheitseinstellungen und/oder Protokolleinstellungen und/oder Benutzer/Gruppenzuordnungen angeben.
4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die Spezifikationsdaten (SD) Relationen zwischen Dateien des Dateisystems angeben.
5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß die Spezifikationsdaten (SD) in einem textuellen und/oder portablen und/oder interoperablen Format vorliegen.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß die Spezifikationsdaten (SD) in XML und/oder in einer Codierung gemäß Codierregeln für ASN.1-definierte Datenstrukturen vorliegen.
- 5
7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß die Spezifikationsdaten (SD) kryptographisch gegen Manipulation und/oder Ausspähung geschützt sind.
- 10 8. Tragbarer Datenträger (10), insbesondere Chipkarte oder Chipmodul, mit einem Prozessorkern (12) und mindestens einem Speicher (14), der dazu eingerichtet ist, ein Verfahren nach einem der Ansprüche 1 bis 7 auszuführen.
- 15 9. Vorrichtung (28) zur Initialisierung und/oder Personalisierung eines tragbaren Datenträgers (10) nach Anspruch 8, die dazu eingerichtet ist, Spezifikationsdaten (SD), die ein in dem tragbaren Datenträger (10) einzurichtendes Dateisystem (26) zumindest zum Teil auf semantischer Ebene beschreiben, an den tragbaren Datenträger (10) zu übertragen.
- 20
10. Computerlesbarer Datenträger (30) mit Spezifikationsdaten (SD), die dazu eingerichtet sind, in einen tragbaren Datenträger (10) eingelesen und dort nach einem Verfahren nach einem der Ansprüche 1 bis 7 interpretiert zu werden.
- 25

1/2

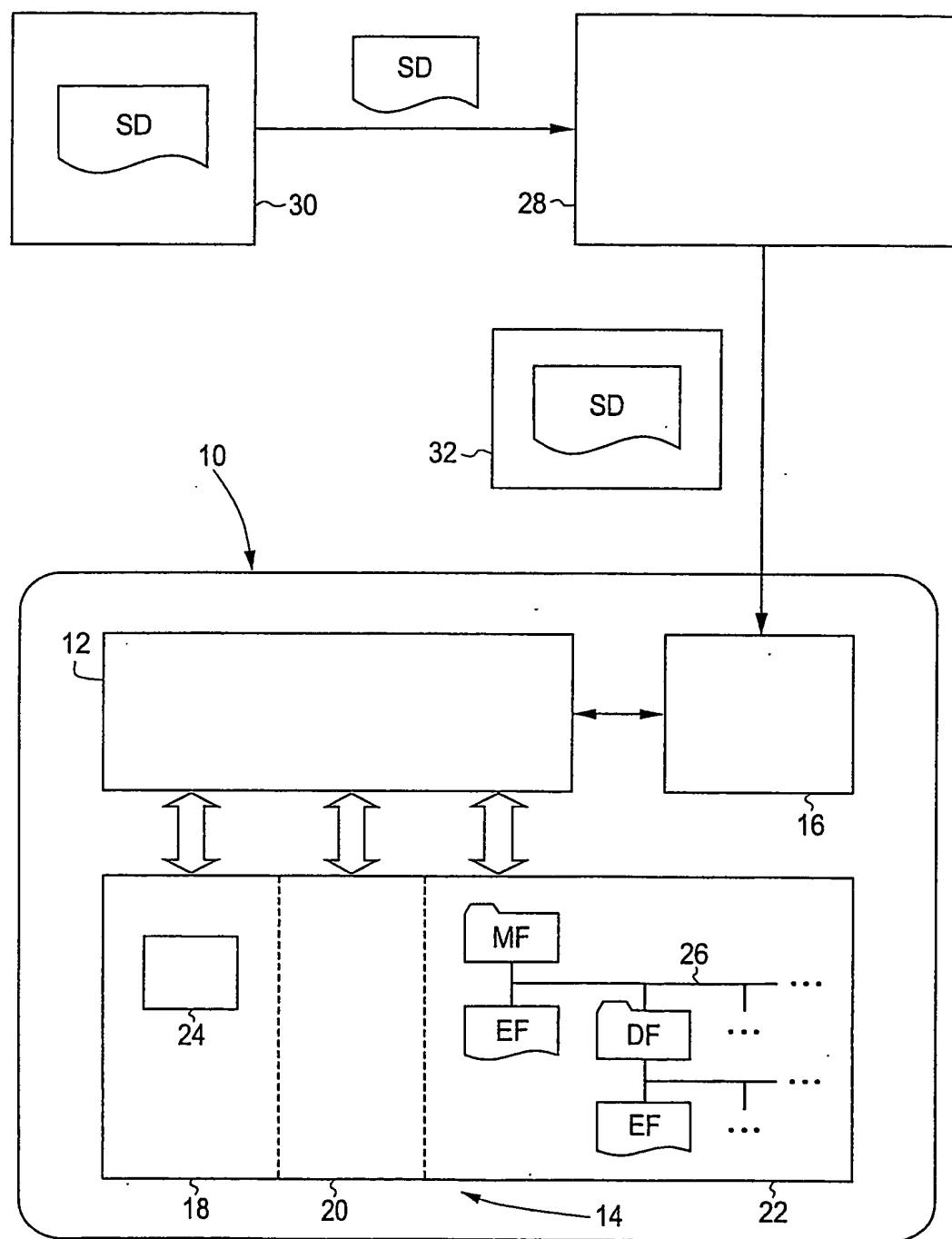


Fig. 1

2/2

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE filesystem SYSTEM "ISO7816.dtd">
<filesystem>
    <Group GroupID="perso" />
    <Group GroupID="users" />
    <Group GroupID="signers" />
    <Group GroupID="webusers" />
    <Personality UserID="Personalisation" PIN="123456"
                  Groups="perso"
                  Options="RemoveAfterLogout" />
    <Personality UserID="Notar" PIN="11111"
                  Groups="users,signers,webusers"
                  Options="LogoutAfterSign" />
    <Personality UserID="Public" PIN="123456" />
<MF>
    <DF AID="#D276000005100C" FID="DF01" access="rw">
        <EF FID="C000" owner="Notar" group="signers"
           mode="rw-r--r--" LinkTo="DF01.ISF.RSA01"
           type="transparent" maxsize="2048" />
        <EF FID="C008" owner="Notar" group="webusers"
           mode="rw-r--r--" LinkTo="DF01.ISF.RSA02"
           type="transparent" maxsize="2048" />
    <ISF>
        <Key KID="01" Type="RSA" Usage="Signhash"
             owner="Notar" group="signers"
             mode="rw-----" />
        <Key KID="02" Type="RSA" Usage="SSL"
             owner="Notar" group="webusers"
             mode="rw-r-----" />
    </ISF>
    </DF>
</MF>
<EXE>
    <EXF EID="genrsa" owner="Personalisation"
         group="users" mode="rw---x---" />
    <EXF EID="signhash" owner="Personalisation"
         group="signers" mode="rw---x---" />
    <EXF EID="sslauth" owner="Personalisation"
         group="webusers" mode="rw---x---" />
</EXE>
</filesystem>
```

Fig. 2

SD

INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 03/08121

A. CLASSIFICATION OF SUBJECT MATTER
 IPC 7 G07F7/10 G06F17/30 G06K19/073

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
 IPC 7 G07F G06F G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)

EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00 68902 A (MICROSOFT CORP) 16 November 2000 (2000-11-16)	9,10
A	page 8, line 4-7 page 13, line 11-19 page 16, line 16 -page 17, line 25 page 21, line 20 -page 22, line 12; figure 4	1-8
A	US 2001/049675 A1 (AZAGURY ALAIN ET AL) 6 December 2001 (2001-12-06) abstract; figures 1,10	1-10
	---	-/-

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

& document member of the same patent family

Date of the actual completion of the international search

3 November 2003

Date of mailing of the international search report

27/11/2003

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Koegler, L

INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 03/08121

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	RANKL, WOLFGANG: "Handbuch der Chipkarten, 3. Auflage" 1999 , CARL HANSER VERLAG , MÜNCHEN WIEN XP002258630 ISBN: 3-446-21115-2 page 222 -page 249 -----	1,3,8,10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 03/08121

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO 0068902	A 16-11-2000	AU 4712000 A		21-11-2000
		EP 1179209 A1		13-02-2002
		WO 0068902 A1		16-11-2000
US 2001049675	A1 06-12-2001	NONE		

INTERNATIONALE RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP 03/08121

A. KLASIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G07F7/10 G06F17/30 G06K19/073

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 G07F G06F G06K

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der Internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, PAJ, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 00 68902 A (MICROSOFT CORP) 16. November 2000 (2000-11-16)	9,10
A	Seite 8, Zeile 4-7 Seite 13, Zeile 11-19 Seite 16, Zeile 16 -Seite 17, Zeile 25 Seite 21, Zeile 20 -Seite 22, Zeile 12; Abbildung 4 ---	1-8
A	US 2001/049675 A1 (AZAGURY ALAIN ET AL) 6. Dezember 2001 (2001-12-06) Zusammenfassung; Abbildungen 1,10 ---	1-10 -/-

Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

Siehe Anhang Patentfamilie

- * Besondere Kategorien von angegebenen Veröffentlichungen :
- *A* Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
- *E* älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
- *L* Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
- *O* Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
- *P* Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

- *T* Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
- *X* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erforderlicher Tätigkeit beruhend betrachtet werden
- *Y* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erforderlicher Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
- *&* Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der Internationalen Recherche

3. November 2003

Absendedatum des Internationalen Recherchenberichts

27/11/2003

Name und Postanschrift der Internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Koegler, L

INTERNATIONALE
FORSCHENBERICHT

Internationales Aktenzeichen

PCT/EP 03/08121

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	RANKL, WOLFGANG: "Handbuch der Chipkarten, 3. Auflage" 1999 , CARL HANSER VERLAG , MÜNCHEN WIEN XP002258630 ISBN: 3-446-21115-2 Seite 222 -Seite 249 -----	1,3,8,10

INTERNATIONALER RECHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP 03/08121

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 0068902	A 16-11-2000	AU 4712000 A EP 1179209 A1 WO 0068902 A1	21-11-2000 13-02-2002 16-11-2000
US 2001049675	A1 06-12-2001	KEINE	